WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Enhancing Cloud Technology Privacy And Security Through Feature Data Sharing

Mohammad Karishma, P.Sathish

Vaageswari College of Engineering,Karimnagar – 505 527, India

ABSTRACT

Storage and retrieval of data can be done remotely via the internet, thanks to cloud computing. Problems with data privacy and access control arise, however, when information is stored on a cloud server that cannot be verified. Due to their inflexibility and lack of fine-grained access control, existing encryption systems like symmetric and asymmetric schemes are unsuitable to provide the access control. Attribute-based encryption is one of the most well-known cryptographic methods for ensuring confidentiality and enabling granular permissions in cloud storage. In this paper, we take a close look at the wide range of access structure and multi-authority ciphertext policy attribute-based encryption schemes currently in use. Additionally, this overview delves deeper into many facets of ciphertext policy attribute-based encryption, including hidden policy, proxy re-encryption, revocation mechanism, and hierarchical attribute - based encryption. Moreover, this research evaluates and contrasts several ABE schemes with regard to their capabilities, safety, and performance. The applicability of attribute-based encryption is also determined in this work. In conclusion, this work compares and contrasts several ABE schemes in order to identify areas of future study and problems that still need to be solved in the field of attribute-based encryption.

KEYWOEDS: Cloud Computing,Data privacy, Privacy, Encryption, Access control, Attribute-based encryption(ABE), authority verification, hidden access policy, privacy preserving.

1. INTRODUCTION

cloud computing:

The term cloud computing refers to the practise of renting out access to various forms of digital infrastructure (including programmes and servers) over the World Wide Web (typically the Internet).

Complex architecture is represented in system diagrams by a cloud-shaped symbol. Data, programmes, and processing are all sent to external services in cloud computing. Cloud computing refers to the use of remotely hosted servers and software applications. Many of these businesses give their customers access to sophisticated server infrastructures and cutting-edge application suites.

· There are consumer-oriented uses for super computing power that were previous for the military and academic institutions. Examples of these include financial portfolios, customize information, data storage, and massively immersive computer games. These application scan perform trillions of calculations per second.

• To divide data processing tasks, the cloud computing uses large groups of computers, often running low-cost consumer PC technology with specialized networking. In today world, the majority of computers are part of a vast network of interconnected devices. Virtualization techniques are routinely used to unlock the full potential of cloud computing.

· It includes: Features and service models:

· Consider these elements of cloud computing, according to NIST definition:

· Rather than dealing with the service providers directly, customers can self-provision computer
resources such as server time and network storage as needed.

· Using standard protocols, any client system no matter how thin or thick, can access network capabilities (e.g., mobile phones, laptops, and PDAs).

· Multi-tenant models allow the providers resources to be pooled to serve many clients, with unique physical and virtual resources dynamically assigned and reassigned according to the demands of the consumers. it is common for customers to be unable or unwilling to know exactly where their purchased goods are located, but may have the option of specifying location at a more abstract level of abstraction (e.g., country, state, or data center).
Resources include virtual machines, storage, processing, and network bandwidth.

The ability to automatically provision and release capabilities in specific situation rapid scaling Out and scaling in. In terms of provision in Clients have seemingly count option to pick from, and they may buy as many as they want any time they want.

· A metering capability at a level of abstraction appropriate to the type of service is used to

automatically control and optimize resource use in cloud computing systems. • (e.g., storage,
processing, bandwidth, and active user accounts). When resources are monitored, controlled and reported on, both service providers and service users profit.

2.OVERVIEW OF CLOUD COMPUTING

Distributed computing is a casual expression used to depict an assortment of various figuring ideas that include countless that are associated through a constant correspondence network (typically the Internet). Distributed computing is a language term without a generally acknowledged non-equivocal logical or specialized definition. In science, distributed computing is an equivalent word for circulated processing over a system and means the capacity to run a program on numerous associated PCs in the meantime. The notoriety of the term can be ascribed to its utilization in advertising to offer facilitated benefits in the feeling of use administration provisioning that run customer server programming on a remote area.

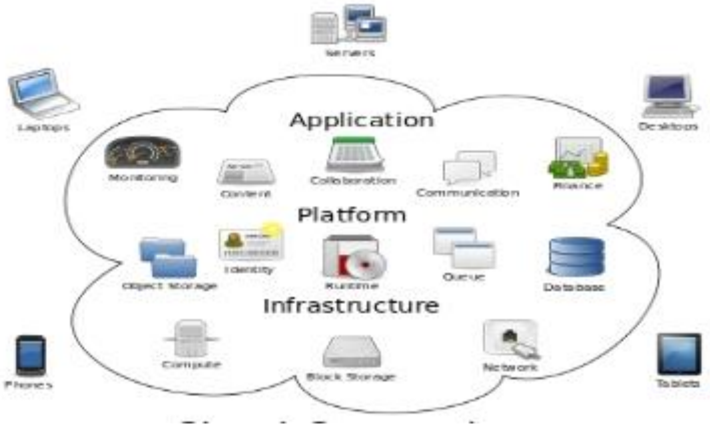

Fig: 2. 1. Cloud Computing

Some Traffic Redundancy Elimination are ushering in the era of distributed computing, which is the expansion and application of computer technology via the Internet. With the advent of Software as a Service (SaaS) registration technology and increasingly affordable and powerful processors, server farms are being transformed into massive data centres with the ability to manage large amounts of data computationally. With ever-faster data transmission rates and more stable but malleable network connections, it is now feasible for customers to subscribe to premium services that rely only on data and applications housed in off-site data centres.

3. RELATED WORK

The software development process is not complete until the literature has been reviewed. Time,money, and resources all need to be calculated before the tool can be created. Once these conditions are met, it is time to move on to the next phase of development: deciding which operating system and programming language will be utilised to create the tool for traffic redundancy elimination.Once development of the tool begins, however, programmers require extensive outside assistance. This assistance is available from seasoned programmers, books, and online resources.
Understanding the following principles is necessary before constructing the system.
1) The state of mobile cloud computing
N. Fernando, S. W. Loke, and W. Rahayu are the authors.
The growing popularity of mobile computing is hampered by the challenges of fully realising its promise, such as limited resources, frequent network outages, and the user's constantly shiftinglocation. Through the use of external resource providers, mobile cloud computing can help with these issues. Here, we highlight the unique challenges of mobile cloud computing and present a comprehensive review of the research in this area. We give a taxonomy of the major problems in this field and explain the many ways in which these problems have been addressed. Finally, we provide a critical analysis of the remaining issues and suggest avenues for future research. Motivation, taxonomies, and open difficulties in mobile cloud-based augmentation Abolfazli, Z. Sanaei, E. Ahmed, A. Gani, and R. Buyya are the authors.Recent years have seen tremendous progress in the use of Cloud-based Mobile Augmentation (CMA) strategies in both academia and industry. In order to facilitate the execution of resource-
intensive mobile apps, the cutting-edge CMA paradigm augments mobile devices with computing power from resource-rich clouds. With the help of external hardware and software, augmented mobile devices can process and store massive amounts of data, going far beyond their native capabilities. Researchers make use of a wide range of cloud-based computing resources (including both far-flung clouds and close-by mobile nodes) to cater to the wide range of computing needs experienced by mobile users. Although using cloud-based computing resources has many benefits, it is not a simple fix. Some of the obstacles that limit CMA adaptability include the complexity of the augmentation process, the diversity of cloud-based resource kinds, and the difficulty of understanding crucial elements (such as the current status of mobile client and remote resources)

that affect on augmentation. This research proposes a taxonomy of CMA methods and conducts an extensive literature review of the mobile augmentation sector. This research aims to address the advantages and disadvantages of using a wide range of cloud-based resources for augmenting mobile devices, as well as to shed light on how the availability of remote resources affects the quality and dependability of augmentation procedures. We provide an overview of what augmentation is, why its useful, and a taxonomy of several kinds of augmentation, both classic and modern, in the cloud and elsewhere. We provide a taxonomy of CMA methods by analysing state-of-the-art methods and categorising them as either far fixed proximate fixed, proximate mobile, or hybrid. An illustrative decision making flowchart for future CMA techniques is shown, along with an introduction to crucial decision making and performance restriction considerations that influence on the adoption of CMA approaches. We address the effects of CMA methods on mobile computing and provide some of the unanswered questions that will guide researchers in the years to come. Thirdly, mobile cloud computing follows industry standards for securing and maintaining mobile cloud ecosystems. R. Kumar and S. Rajalakshmi are the authors. Cloud computing ideas mesh easily with mobile devices to provide convenient, always-available services. It is anticipated that the growth of the mobile ecosystem will be facilitated by the emergence of mobile cloud computing as a significant subset of cloud computing. Undoubtedly, security concerns will increase in tandem with the proliferation and development of mobile devices.A second factor that will increase the importance of Internet security is the exponential increase in the number and variety of Internet-connected devices. Customers and businesses alike are understandably concerned about the genuine potential of mobile cloud computing and the identification of difficulties with mobile cloud security, privacy, feasibility, and accessibility. This paper examines the state of cloud security breaches, the vulnerabilities of mobile cloud devices, and the best practises for addressing those vulnerabilities in future research on mobile device management and mobile data protection, all of which contribute to the mobile cloud security issues and challenges discussed in this paper. In addition, it emphasises the use of SCWS (Smart Card Web Services) competition to strengthen mobile cloud computing security.

4) A smart and intelligent world is the result of mobile cloud sensing, big data, and 5G networks.

THE AUTHORS: Q. Han, S. Liang, and H. Zhang

Mobile phones have evolved over time to become more sophisticated tools that can perform a wide variety of functions and satisfy a wide range of user requirements. Whether it be a personal need for a health care manager or a more abstract one for a monitor of the environment, there is a wide variety of services that people require. As a result, the introduction of mobile phones has improved the quality of our daily lives in many ways. After introducing the concepts of mobile sensing and cloud computing independently, we will merge them into a single idea: mobile cloud sensing. We will also examine each component of mobile cloud sensing and provide an intuitive architectural description of the technology. Today, mobile cloud sensing has its limitations, but with the advent of 5G and the analysis of large data, we can solve these problems. We anticipate further improvement in all aspects of our lives thanks to the development of mobile cloud sensing, 5G networks, and big data processing.Access Control in Distributed Systems: Integrating Theory and Practice 5 AUTHORED BY: I. Stojmenovic Through the use of authentication and authorization procedures, only approved users are granted access to systems and resources. In distributed systems, where a centralised authority coordination of actions could be impossible or resource-demanding, this issue becomes more difficult to solve.Newer cryptographic primitives are being implemented for access control, one of which is called Attribute Based Encryption (ABE). This paper discusses some recent issues with access control in distributed systems, including mobile ad hoc networks, vehicular networks, smart grids, and the cloud. Various limitations and prerequisites are placed on each of these uses. We demonstrate how ABE and its many versions can be adapted to meet the requirements of the aforementioned uses.

4.METHODOLOGY:

DATA OWNER:

In this module, data owner has to register to Authentication Center and Authentication Center checks and authorizes the data owner login. Data owner browse the file, encrypt and upload file with its mac. Once uploaded the file all the authentication center must provide the storage access for the file store on the cloud. Data owner can also delete the file after the uploading of the file to the cloud.

Authentication Center

In this module Authentication Center checks user & owner login and authorizes the registration. Authentication center list all other sub-authentication centers and provide authorization (Activate OR Deactivate). Authentication center provides the storage access to cloud for every file uploaded by the data owner.

AA 1

In this module the AA1 shows all the private key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

AA 2

In this module the AA2 shows all the public key requests from the users and generates. And also provides the storage access for the file uploaded by the data owner.

Cloud Server

Receive all files from the data owner and store all files, user details. Provide files to end user after verifying Private key and secret key provided by the authentication center. Maintain file transaction details and forward the file download request from the user to the authentication centre.

End User (Receiver)

In this module end user has to register and login, and the user is authorized by the authentication Center, user will request private key from the AA1 and the secret key from the AA2 to download the file from cloud server

5. CONCLUSION

We put forth a CP-ABE strategy in the canonical setting that protects user anonymity. Some of the benefits of the proposed approach include constant-size private keys and compact ciphertexts, neither of which are features of the previous schemes. Moreover, only four pairing computations are required for decryption. In a group of prime order, the suggested approach provides both selective security an anonymity. We demonstrate that the suggested scheme's security can be boiled down to the decisional n-BDHE and the DL assumptions in the standard model. In addition, the suggested approach allows for the verification of authorities without compromising users' confidentiality. The provided approach, however, is only capable of "AND" policy, and it is based on a flimsy security paradigm. Future research should focus on how to build a more secure, flexible HP-CP-ABE scheme.

.REFERENCES

[1] Li, S. Yu, K. Ren, and W. Lou, "Securing personal health records In cloud computing :Patient- M centric and fine-grained data access control in multi-owner settings," in Security and Privacy in Communication Networks. Springer, 2010, pp.89–106.

[2] A. M.-H. Kuo, "Opportunities and challenges of cloud computing To improve healthcare services," Journal of medical Internet research, vol.13, no.3,2011.

[3] M. Li, S. Yu, Y. Zheng, K. Ren, and W. Lou, "Scalable and secure sharing of personal health
records in cloud computing using attribute-based encryption," IEEE Transactions on Parallel and Distributed Systems, vol.24,no.1,pp.131–143,2013.

[4] L. M. Vaquero, L.-Merino, J. Caceres, and M. Lindner, "A breaking the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol.39,no.1,pp.50–55,2008.

[5] H. Liang, L. X. Cai, D. Huang, X. Shen, and D. Peng, "An based service model for inter domain resource allocation in mobile cloud networks," IEEE Transactions logy,vol.61,no.5,pp.22222232,2012.

[6] M. M. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," IEEE Transactions on Parallel and Distributed Systems, vol. 23, no. 10, pp. 1805–1818,2012.

[7] Q. Shen, X. Liang, X. Shen, X. Lin, and H. Luo, "Exploiting geo distributed clouds for e-health monitoring system with minimum service delay and privacy preservation," IEEE Journal of Biomedical and Health Informatics,vol.18,no.2 ,pp.430–439,2014.

[8] C. Wang, N. Cao, K. Ren, and W. Lou, "Enabling secure and efficient ranked keyword search over outsourced cloud data," IEEE Transactions on Parallel and Distributed Systems,vol.23,no.8,pp.1467–1479,2012.

[9] W. Sun, B. Wang, N. Cao, M. Li, W. Lou, Y. T. Hou, and H. Li, "Verifiable privacy-
preserving multi-keyword text search in the cloud supporting similarity-based ranking," IEEE Transactions on Parallel and Distributed Systems,vol.25,no.11,pp.3025–3035,2014.

[10] J. Yu, P. Lu, Y. Zhu, G. Xue, and M. Li, "Towards secure multi-keyword top-k retrieval over encrypted cloud data," IEEE Transactions on Dependable and Secure Computing,vol.10,no.4,pp.239–250,2013.